WHAT IS CLAIMED IS:

1. A microprocessor internally having a secret key specific to the microprocessor that cannot be read out to an external, the microprocessor comprising:

a processor core configured to execute instructions of a program including plaintext instructions and encrypted instructions, the encrypted instructions being encrypted by using an instruction key specific to the program; and

a key management unit configured to carry out a key registration for reading out from an external memory a distribution key that is obtained in advance by encrypting the instruction key by using a public key corresponding to the secret key, decrypting the distribution key by using the secret key to obtain the instruction key, and registering the instruction key in correspondence to a specific program identifier for identifying the program into a key table, and to notify a completion of the key registration to the processor core asynchronously by interruption when the key registration is completed, such that the key management unit carries out the key registration during execution of the program by the processor core in which execution of the encrypted instructions starts after the completion of the key registration is notified.

2. The microprocessor of claim 1, further comprising:

an instruction cache memory configured to store a cache line containing a part of the instructions of the program in correspondence to the specific program identifier, and permit reading of the cache line only when the specific program identifier stored in correspondence to the cache line coincides with a program identifier received along with a program reading request from the processor core;

wherein the key management unit is also configured to carry out a flashing of the cache line stored in correspondence to the specific program identifier on the cache memory when the key management unit rewrites the instruction key corresponding to the specific program identifier in the key table.

3. The microprocessor of claim 2, wherein the key management unit carries out the flashing in parallel to the key registration, and notifies the completion of the key registration to the processor core when the key registration and the flashing are both completed.

4. The microprocessor of claim 1, further comprising:

an instruction decryption processing unit configured to decrypt the encrypted instructions of the program read out from the external memory, by using the instruction key registered in correspondence to the specific program identifier by the key management unit, according to a chain information indicating chain relationships among encryption blocks in units of which the encrypted instructions are encrypted.

5. The microprocessor of claim 1, wherein the key management unit is also configured to register a data key to be used in encrypting/decrypting data for the program in correspondence to the specific program identifier into the key table.

6. The microprocessor of claim 5, wherein the key table stores a plurality of instruction keys or data keys which are indexed by key value indexes, and the microprocessor further comprises:

a key index conversion unit configured to convert a set of a program identifier and a key type identifier

received from the processor core into a corresponding key value index; and

a decryption processing unit configured to decrypt encrypted instructions or data of a program specified by the program identifier received from the processor core and read out from the external memory, by using an instruction key or a data key indexed by the corresponding key value index obtained by the key index conversion unit.

7. The microprocessor of claim 6, wherein the key index conversion unit converts more than one sets of a program identifier and a key type identifier into an identical key value index.

8. The microprocessor of claim 6, further comprising:

a cache memory configured to store a part of instructions or data of programs by using key value indexes obtained by the key index conversion unit as cache tags.

9. The microprocessor of claim 1, wherein the key management unit is also configured to register a context key to be used in encrypting/decrypting context for the program in correspondence to the specific program identifier into the key table.

10. A microprocessor internally having a secret key specific to the microprocessor that cannot be read out to an external, the microprocessor comprising:

a processor core configured to execute instructions of a program including plaintext instructions and encrypted instructions, the encrypted instructions being encrypted by using an instruction key specific to the program; and

a key management unit configured to carry out a key registration for reading out from an external memory a distribution key that is obtained in advance by encrypting

the instruction key and a meta-level information integrally by using a public key corresponding to the secret key, decrypting the distribution key by using the secret key to obtain the instruction key and the meta-level information, and registering the instruction key and the meta-level information in correspondence to a specific program identifier for identifying the program into a key table.

11. The microprocessor of claim 10, wherein the key management unit registers the meta-level information which is a feedback key to be used in obtaining a feedback information by encrypting the instruction key when the feedback information is to be written into the external memory at a time of a context saving.

12. The microprocessor of claim 10, wherein the key management unit registers the meta-level information which is a perpetuation flag indicating whether or not to permit a context saving in which the instruction key is encrypted by using a prescribed secret key of the microprocessor and written into the external memory.